

Skew Cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ *

Ting YAO, Minjia SHI

School of Mathematical Sciences of Anhui University, China

Patrick SOLÉ

Telecom Paris Tech, France and King Abdulaziz University, Saudi Arabia

Abstract: In this paper, we study skew cyclic codes over the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu, q = p^m$ and p is an odd prime. We investigate the structural properties of skew cyclic codes over R through a decomposition theorem. Furthermore, we give a formula for the number of skew cyclic codes of length n over R .

Key words: linear codes; skew cyclic codes; Gray map; generator polynomial

MSC (2010) : Primary 94B15; Secondary 11A15.

1 Introduction

Cyclic codes form an important subclass of linear block codes, studied from the fifties onward. Their clear algebraic structures as ideals of a quotient ring of a polynomial ring makes for an easy encoding. A landmark paper [11] has shown that some important binary nonlinear codes with excellent error-correcting capabilities can be identified as images of linear codes over \mathbb{Z}_4 under the Gray map.

Recently, in [3], D. Boucher et al. gave skew cyclic codes defined by using the skew polynomial ring with an automorphism θ over the finite field with q elements. The definition generalizes the concept of cyclic codes over non-commutative polynomial rings. Soon afterwards, D. Boucher et al. studied skew constacyclic codes in [5]. Later, in [4], some important results on the duals of the skew cyclic codes over $\mathbb{F}_q[x; \theta]$ are given. In [12], I. Siap et al. presented the structure of skew cyclic codes of arbitrary length. Further, S. Jitman et al. in [10] defined skew constacyclic codes over the skew polynomial ring with coefficients from finite rings. In [1], T. Abualrub and P. Seneviratne studied skew cyclic codes over ring $\mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$. Moreover, J. Gao [6] and F. Gursoy et al. [8] presented skew cyclic

*Corresponding author: Minjia Shi. **The original manuscript was first submitted for reviewing on 4nd December 2014.** This research is supported by NNSF of China (61202068), Talented youth Fund of Anhui Province Universities (2012SQRL020ZD).

codes over $\mathbb{F}_p + v\mathbb{F}_p$ and $\mathbb{F}_q + v\mathbb{F}_q$ with different automorphisms, respectively. In [7], J. Gao et al. also studied skew generalized quasi-cyclic codes over finite fields.

In this article, we mainly study skew cyclic codes over ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu$ and $q = p^m$.

In our work, the automorphism θ on the ring R is defined to be

$$\theta(b_0 + b_1u + b_2v + b_3uv) = b_0^p + b_2^p u + b_1^p v + b_3^p uv,$$

for all $b_0 + b_1u + b_2v + b_3uv \in R$, where $b_i \in \mathbb{F}_q$, and $i = 0, 1, 2, 3$. In fact, for any $a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4 \in R$, we have

$$\theta(a_1\eta_1 + a_2\eta_2 + a_3\eta_3 + a_4\eta_4) = \theta(a_1)\eta_1 + \theta(a_2)\eta_2 + \theta(a_3)\eta_3 + \theta(a_4)\eta_4.$$

Note that if m is even, the order of the ring automorphism $|\langle\theta\rangle|$ is m , otherwise, $2m$.

The material is organized as follows. In Section 2, we show the basics of codes over ring R that we need for further reference. Section 3 derives the structure of linear codes over R . In Section 4, we introduce skew cyclic codes over ring R and give the structural properties of skew cyclic codes over R through a decomposition theorem. Section 5, we give an example to illustrate the discussed results.

2 Preliminary

Let \mathbb{F}_q be a finite field with q elements, where $q = p^m$, p is an odd prime. Throughout, we let R denote the commutative ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v$, and $uv = vu$. Let $\eta_1 = 1 - u - v + uv$, $\eta_2 = uv$, $\eta_3 = u - uv$, $\eta_4 = v - uv$. It is easy to verify that $\eta_i^2 = \eta_i, \eta_i\eta_j = 0$, and $\sum_{k=1}^4 \eta_k = 1$, where $i, j = 1, 2, 3, 4$, and $i \neq j$. According to [2], we have $R = \eta_1 R \oplus \eta_2 R \oplus \eta_3 R \oplus \eta_4 R$. By calculating, we can easily obtain that $\eta_i R \cong \mathbb{F}_q$, $i = 1, 2, 3, 4$. Therefore, for any $r \in R$, r can be expressed uniquely as $r = \sum_{i=1}^4 \eta_i a_i$, where $a_i \in \mathbb{F}_q$ for $i = 1, 2, 3, 4$.

We recall the definition of the Gray map over R in [13]

$$\begin{aligned} \Phi : R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q &\rightarrow \mathbb{F}_q^4 \\ \eta_1 a + \eta_2 b + \eta_3 c + \eta_4 d &\rightarrow (a, a + b, a + c, a + b + c + d). \end{aligned}$$

Equivalently, if $r = a' + b'u + c'v + d'uv \in R$, then

$$\Phi(r) = (a', 2a' + b' + c' + d', 2a' + b', 4a' + 2b' + 2c' + d').$$

This map can be naturally extended to the case over R^n .

For any element $r = a + bu + cv + duv \in R$, we define the Lee weight of r as $w_L(r) = w_H(a, a + b, a + c, a + b + c + d)$, where w_H denotes the ordinary Hamming weight for q -ary codes. The Lee distance of $r \in R$ can be similarly defined.

From the definition of the Gray map Φ , we can easily check that Φ is \mathbb{F}_q -linear and it is also a distance-reserving isometry from (R^n, d_L) to (F_q^{4n}, d_H) , where d_L and d_H denote the Lee and Hamming distance in R^n and F_q^{4n} , respectively.

3 Linear codes over R

In this section, we mainly show some familiar structural properties of R . The proofs of the following theorems can be found in [13], so we omit them here.

If A_i ($i = 1, 2, 3, 4$) are codes over R , we denote their direct sum by

$$A_1 \oplus A_2 \oplus A_3 \oplus A_4 = \{a_1 + a_2 + a_3 + a_4 | a_i \in A_i, i = 1, 2, 3, 4\}.$$

Definition 3.1 Let C be a linear code of length n over R , we define that

$$C_1 = \{\mathbf{a} \in \mathbb{F}_q^n | \exists \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n | \eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c} + \eta_4 \mathbf{d} \in C\},$$

$$C_2 = \{\mathbf{b} \in \mathbb{F}_q^n | \exists \mathbf{a}, \mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n | \eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c} + \eta_4 \mathbf{d} \in C\},$$

$$C_3 = \{\mathbf{c} \in \mathbb{F}_q^n | \exists \mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_q^n | \eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c} + \eta_4 \mathbf{d} \in C\},$$

$$C_4 = \{\mathbf{d} \in \mathbb{F}_q^n | \exists \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n | \eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c} + \eta_4 \mathbf{d} \in C\}.$$

It is clear that C_i ($i = 1, 2, 3, 4$) are linear codes over \mathbb{F}_q^n . Furthermore, $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$, and $|C| = |C_1| \cdot |C_2| \cdot |C_3| \cdot |C_4|$. Throughout the paper C_i ($i = 1, 2, 3, 4$) will be reserved symbols referring to these special subcodes.

According to Definition 3.1 and [13], we have the following theorem.

Theorem 3.1 Let $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$ be a linear code of length n over R . Then $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp \oplus \eta_4 C_4^\perp$.

According to the definition of the Gray map Φ , we can easily obtain the following theorem.

Theorem 3.2 Let C be a linear code of length n over R , $|C| = q^k$ and $d_L(C) = d$. Then $\Phi(C)$ is a q -ary linear code with parameter $[4n, k, d]$.

Let $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$ be a linear code of length n over R . Since C is a F_q -module, then we have the following lemma.

Lemma 3.1 If G_i are generator matrices of q -ary linear codes C_i ($i = 1, 2, 3, 4$), respectively, then the generator matrix of C is

$$G = \begin{pmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \\ \eta_4 G_4 \end{pmatrix}.$$

Moreover, if $G_1 = G_2 = G_3$, then $G = G_1$.

In light of the definition of Gray map Φ , we can easily obtain the following proposition.

Proposition 3.1 If C is a linear code of length n over R with generator matrix G , then we have

$$\Phi(G) = \begin{pmatrix} \Phi(\eta_1 G_1) \\ \Phi(\eta_2 G_2) \\ \Phi(\eta_3 G_3) \\ \Phi(\eta_4 G_4) \end{pmatrix} = \begin{pmatrix} G_1 & G_1 & G_1 & G_1 \\ \mathbf{0} & G_2 & \mathbf{0} & G_2 \\ \mathbf{0} & \mathbf{0} & G_3 & G_3 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & G_4 \end{pmatrix}.$$

4 Skew Cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$

In this section, we assume C_3 and C_4 are equivalent. Before studying skew cyclic codes over R , we define a skew polynomial ring $R[X; \theta]$ and skew cyclic codes over R . Next, we determine the structural properties of skew cyclic codes over R through a decomposition theorem.

Definition 4.1 We define the skew polynomial ring as $R[x; \theta] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, i = 0, 1, \dots, n\}$, where the coefficients are written on the left of the variable x . The multiplication is defined by the basic rule $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$, and the addition is defined to be the usual addition rule of polynomials.

It is easily checked that the ring $R[x; \theta]$ is not commutative unless θ is the identity automorphism on R .

Definition 4.2 A nonempty subset C of R^n is called a skew cyclic code of length n if C satisfies the following conditions: (1) C is a submodule of R^n ; (2) if $r = (r_0, r_1, \dots, r_{n-1}) \in C$, then skew cyclic shift $\rho(r) = (\theta(r_{n-1}), \theta(r_0), \dots, \theta(r_{n-2})) \in C$.

Theorem 4.1 Let $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$ be a linear code of length n over R , where C_i ($i = 1, 2, 3, 4$) are codes over \mathbb{F}_q of length n . Then C is a skew cyclic code with respect to the automorphism θ if and only if C_i are skew cyclic codes over \mathbb{F}_q with respect to the automorphism θ .

Proof For any $r = (r_0, r_1, \dots, r_{n-1}) \in C$, let $r_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i + \eta_4 d_i$ for $0 \leq i \leq n-1$, where $a = (a_0, a_1, \dots, a_{n-1}) \in C_1$, $b = (b_0, b_1, \dots, b_{n-1}) \in C_2$, $c = (c_0, c_1, \dots, c_{n-1}) \in C_3$

and $d = (d_0, d_1, \dots, d_{n-1}) \in C_4$. If C_i are skew cyclic codes, then $\rho(r) = \rho(\eta_1 a + \eta_2 b + \eta_3 c + \eta_4 d) = \eta_1 \rho(a) + \eta_2 \rho(b) + \eta_3 \rho(c) + \eta_4 \rho(d) \in C$. This implies that C is a skew cyclic code over R .

On the other hand, if C is a skew cyclic code over R , we have $\rho(r) = (\theta(r_{n-1}), \theta(r_0), \dots, \theta(r_{n-2})) = \eta_1 \rho(a) + \eta_2 \rho(b) + \eta_3 \rho(c) + \eta_4 \rho(d) \in C$, which implies $\rho(a) \in C_1$, $\rho(b) \in C_2$, $\rho(c) \in C_3$, $\rho(d) \in C_4$. Thus C_i are skew cyclic codes over \mathbb{F}_q .

According to [4, Corollary 18], we know that the dual code of every skew cyclic code over \mathbb{F}_q is also skew cyclic. By using this connection and Theorem 4.1, we get the following corollary.

Corollary 4.1 If C is a skew cyclic code over R , then the dual code C^\perp is also skew cyclic.

The following theorem determines the generator polynomials of a skew cyclic code of length n over R .

Theorem 4.2 Let $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$ be a skew cyclic code of length n over R and suppose that $g_i(x)$ are generator polynomials of C_i ($i=1, 2, 3, 4$) respectively. Then $C = \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle$ and $|C| = q^{4n - \sum_{i=1}^4 \deg(g_i(x))}$.

Proof Since $C_i = \langle g_i(x) \rangle$, for $i = 1, 2, 3, 4$, and $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$, then

$$C = \left\{ c(x) = \sum_{i=1}^4 \eta_i r_i(x) g_i(x) \mid r_i(x) \in \mathbb{F}_q[x; \theta] \right\}.$$

Hence $C \subseteq \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle$. Conversely, for any $\sum_{i=1}^4 \eta_i k_i(x) g_i(x) \in \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle$, where $k_i(x) \in R[x; \theta]/(x^n - 1)$, then there exist $r_i \in \mathbb{F}_q[x; \theta]$ such that $\eta_i k_i(x) = \eta_i r_i(x)$, $i = 1, 2, 3, 4$. Thus $\langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle \subseteq C$, which implies $C = \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle$. Since $|C| = |C_1| \cdot |C_2| \cdot |C_3| \cdot |C_4|$, we obtain that $|C| = q^{4n - \sum_{i=1}^4 \deg(g_i(x))}$.

Theorem 4.3 Let C_i ($i = 1, 2, 3, 4$) be skew cyclic codes over \mathbb{F}_q and $g_i(x)$ be the monic generator polynomials of these codes respectively, then there is a unique polynomial $g(x) \in R[x; \theta]$ such that $C = \langle g(x) \rangle$ and $g(x)$ is a right divisor of $x^n - 1$, where $g(x) = \sum_{i=1}^4 \eta_i g_i(x)$.

Proof By Theorem 4.2, we know $C = \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x), \eta_4 g_4(x) \rangle$. We take $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x) + \eta_4 g_4(x)$, obviously, we have $\langle g(x) \rangle \subseteq C$. On the other hand, one can check that $\eta_i g_i(x) = \eta_i g(x)$ ($i = 1, 2, 3, 4$), which implies $C \subseteq \langle g(x) \rangle$. Hence $C = \langle g(x) \rangle$. Since $g_i(x)$ are monic right divisors of $x^n - 1 \in \mathbb{F}_q[x; \theta]$, then there exist

$r_i(x) \in \mathbb{F}_q[x; \theta]$ such that $x^n - 1 = r_i(x)g_i(x)$. Thus

$$\begin{aligned}
[\eta_1 r_1(x) + \eta_2 r_2(x) + \eta_3 r_3(x) + \eta_4 r_4(x)]g(x) &= \sum_{i=1}^4 \eta_i r_i(x) \cdot \sum_{i=1}^4 \eta_i g_i(x) \\
&= \sum_{i=1}^4 \eta_i r_i(x) g_i(x) \\
&= \sum_{i=1}^4 \eta_i (x^n - 1) \\
&= x^n - 1.
\end{aligned}$$

This implies $g(x)$ is a right divisor of $x^n - 1$.

Corollary 4.2 Every left submodule of $R[x; \theta]/(x^n - 1)$ is principally generated.

Let $g(x) = g_0 + g_1x + \cdots + g_tx^t$ and $h(x) = h_0 + h_1x + \cdots + h_{n-t}x^{n-t}$ be polynomials in $\mathbb{F}_q[x; \theta]$ such that $x^n - 1 = h(x)g(x)$ and C be the skew cyclic code generated by $g(x)$ in $\mathbb{F}_q[x; \theta]/(x^n - 1)$, according to Corollary 18 in [4], then the dual code of C is a skew cyclic code generated by $\tilde{h}(x) = h_{n-t} + \theta(h_{n-t-1})x + \cdots + \theta^{n-t}(h_0)x^{n-t}$. Therefore we have the following corollary.

Corollary 4.3 Let C_i be skew cyclic codes over \mathbb{F}_q and $g_i(x)$ be their generator polynomial such that $x^n - 1 = h_i(x)g_i(x)$ in $\mathbb{F}_q[x; \theta]$. If C is a skew cyclic code over R , then $C^\perp = \langle \sum_{i=1}^4 \eta_i \tilde{h}_i(x) \rangle$ and $|C^\perp| = q^{\sum_{i=1}^4 \deg(g_i(x))}$.

In light of previous introduction, we know that the order of θ is even. Therefore, we always assume that n be odd in the rest of the paper.

Theorem 4.4 [6] Let n be odd and C be a skew cyclic code of length n , then C is equivalent to a cyclic code of length n over R .

By Theorem 4.4, we can determine the number of distinct skew cyclic codes of odd length n over R .

Corollary 4.4 Let n be odd and $x^n - 1 = \prod_{i=1}^r p_i^{s_i}(x)$, where $p_i(x) \in F_q[x; \theta_i]$ is irreducible, then the number of distinct skew cyclic codes of length n over R is equal to the number of ideals in $R[x]/(x^n - 1)$, i.e. $\prod_{i=1}^r (s_i + 1)^4$.

5 Application Examples

In this section, we will exhibit a example of skew cyclic codes and their Gray images over $GF(9)$. Before giving a example, we first give the definition of Plotkin Sum.

Let $C \oplus_P D$ denote the Plotkin sum of two linear codes C and D , also called $(u|u + v)$ construction, where $u \in C, v \in D$. For more information on the Plotkin sum, one can see a

good survey [9].

In the following, we assume G_i are generator matrices of 9-ary linear codes C_i for $i = 1, 2, 3, 4$, respectively. Let $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4$ be a linear code of length n over R , then its Gray image $\Phi(C)$ is none other than

$$(C_1 \oplus_P C_2) \oplus_P (C_3 \oplus_P C_4).$$

We construct skew cyclic codes over $GF(9)$ with some conditions. If C_1 is a $[20, 1, 20]$ code, C_2 is a $[20, 9, 4]$ code, C_3 is a $[20, 10, 2]$ code and C_4 is a $[20, 10, 2]$ code, then the Gray image of C has parameters $[80, 30, 4]$ over $GF(9)$.

6 Conclusion

This paper is devoted to studying skew cyclic codes over $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu, q = p^m$ and p is an odd prime. First, we introduce the structure of linear codes over R and show the structural properties of skew cyclic codes over R . Next, we give the enumeration of distinct skew cyclic codes over R when n is odd.

References

- [1] T. Abualrub, P. Seneviratne. Skew codes over rings. IMECS, Hong Kong, 2012, (2).
- [2] F. W. Anderson, K. R. Fuller. Rings and categories of modules. Springer, 1992.
- [3] D. Boucher, W. Geiselmann, F. Ulmer. Skew cyclic codes. Appl. Algebra Eng. Comm, 2007, 18(4): 379-389.
- [4] D. Boucher and F. Ulmer. Coding with skew polynomial ring. J. Symb. Comput., 2009, 44(12): 1644-1656.
- [5] D. Boucher, P. Solé, F. Ulmer. Skew constacyclic codes over Galois ring. Adv. in Math. of Comm., 2008, 2(3): 273-292.
- [6] J. Gao. Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. J. Appl. Math. Inform. 2013, 31: 337-342.
- [7] J. Gao, L. Z. Shen, F. W. Fu. Skew Generalized Quasi-Cyclic Codes over Finite Fields. arXiv preprint arXiv:1309.1621, 2013.
- [8] F. Gursoy, I. Siap and B. Yildiz. Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. Advances in Mathematics of Communications, 2014, 8(3): 313-322.
- [9] F. Hernando, D. Ruano. Sixteen New Linear Codes With Plotkin Sum. arXiv preprint arXiv:0804.3507, 2008.
- [10] S. Jitman, S. Ling, P. Udomkavanich. Skew constacyclic over finite chain rings. Adv. Math. Commum. 2012, 6(1): 29-63.

- [11] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé. The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Coethals, and related codes. *IEEE Trans. Inform. Theory*, 1994, 40(2): 301-319.
- [12] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne. Skew cyclic codes of arbitrary length. *Int. Nat. Sci.*, 2011, 2(1): 10-20.
- [13] Y. T. Zhang. Research on Constacyclic Codes over Some Classes of Finite Non-chain Rings, Master's thesis. Hefei university of technology, 2013.